RANCANG BANGUN SISTEM KEAMANAN LAPIS GANDA UNTUK OTOMATISASI PEMBLOKIRAN IP PENYERANG BERBASIS
FAIL2BAN DAN API MIKROTIK PADA REVERSE PROXY NGINX DI LINGKUNGAN VIRTUALISASI PROXMOX PT GLOBAL
INTERMEDIA NUSANTARA
Munif Adam Ashidiqi, Ir. Muhammad Arrofiq, S.T., M.T., Ph.D., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR ISI

LEMBAR PENGESAHAN iii
PERNYATAAN BEBAS PLAGIASI iv
KATA PENGANTAR v
DAFTAR ISI vii
DAFTAR GAMBAR ix
DAFTAR TABEL xii
DAFTAR SIMBOL xiii
INTISARI xiv
***ABSTRACT* ..... xv**
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Tujuan dan Manfaat Proyek Akhir 3
1.3.1 Tujuan 3
1.3.2 Manfaat 3
1.4 Batasan Penelitian 3
1.5 Sistematika Penulisan 5
BAB II KAJIAN PUSTAKA 6
2.1 Tinjauan Pustaka 6
2.2 Dasar Teori 14
2.2.1 *Proxmox Virtual Evironment* 14
2.2.2 Mikrotik RouterOS 15
2.2.3 Konsep Pertahanan Berlapis (*Defense in Depth*) 16
2.2.4 Peran Reverse Proxy dalam Keamanan Layanan *Web* 16
2.2.5 Penggunaan Fail2ban untuk Pemblokiran Otomatis 17
2.2.6 Pemanfaatan API RouterOS untuk Otomatisasi *Firewall* 17
2.2.7 Integrasi Komponen untuk Sistem Pertahanan Berlapis 18
Hubungan dengan Proyek 18
2.3 Hipotesis 19
BAB III METODE PENELITIAN 20

RANCANG BANGUN SISTEM KEAMANAN LAPIS GANDA UNTUK OTOMATISASI PEMBLOKIRAN IP PENYERANG BERBASIS
FAIL2BAN DAN API MIKROTIK PADA REVERSE PROXY NGINX DI LINGKUNGAN VIRTUALISASI PROXMOX PT GLOBAL
INTERMEDIA NUSANTARA
Munif Adam Ashidiqi, Ir. Muhammad Arrofiq, S.T., M.T., Ph.D., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

3.1 Alat dan Bahan 20
3.2 Tahapan proyek akhir 22
3.3 Perancangan Sistem 24
3.3.1 Topologi Jaringan 24
3.3.2 Daftar Alamat IP 26
3.3.3 Persiapan Infrastruktur Virtual pada Proxmox 26
3.4 Implementasi 31
3.4.1 Konfigurasi Dasar Mikrotik CHR dan Jaringan Internal 31
3.4.2 Konfigurasi Nginx Reverse Proxy dan DNS 36
3.4.3 Instalasi dan Konfigurasi Sistem Keamanan 49
3.4.4 Integrasi API Mikrotik dengan Python 57
3.5 Pengujian Sistem 63
3.5.1 Pengujian Serangan *Scanning* 64
3.5.2 Pengujian Serangan *Brute Force* 67
3.5.3 Pengujian Serangan *SQL Injection* 69
3.5.4 Pengujian Serangan *Denial of Service* 72
BAB IV HASIL DAN PEMBAHASAN 75
4.1 Hasil Pengujian Serangan *Scanning* 75
4.2 Hasil Pengujian Serangan *Brute Force* 77
4.3 Hasil Pengujian Serangan *SQL Injection* 80
4.4 Hasil Pengujian Serangan *DoS* 82
4.5 Evaluasi Keberhasilan Sistem 84
BAB V PENUTUP 86
5.1 Kesimpulan 86
5.2 Saran 87
DAFTAR PUSTAKA 88
LAMPIRAN 91